EXHIBIT 10

Redacted Version of Document Sought to be Sealed

Message

From: Tom Bergan [tombergan@google.com]
Sent: 9/13/2019 7:12:32 PM
To: Paul Jensen [pauljensen@google.com]
CC: IP address privacy [ip-address-privacy@google.com]
Subject: Re: Willful IP Blindness

Very intriguing proposal. I like how this lays the groundwork for Google running a privatizing proxy with community auditing and oversight, especially since I'm not sure anyone besides Google is able or willing to run such a proxy at full internet scale. Since this will be public, I tried to read the explainer from the perspective of someone who knows nothing about [redacted] other than the existing public explainers. Feedback from this perspective:

First, it's not clear how much Privacy Budget is consumed by an IP address. Since IP addresses often uniquely identify users, I assume the answer should be "all of the budget", yet the explainer has phrases like "what [budget] remains after IP address access is deducted". It's difficult to understand the long-term vision without understanding this answer. The explainer would benefit from a section like this one.

Second, the explainer doesn't define "universal IP privacy" and doesn't explain how to hide an IP address from a server while also making the IP address available for DoS and SPAM detection.

Third, people concerned about privacy are mostly concerned about Big Ads, and Big Ads are mostly not hosted behind "public CDNs". The implied long-term vision seems to be that all tracking/ads servers are: (a) moved behind an audited CDN, or (b) fronted by an audited proxy, or (c) blocked entirely. If that is a correct interpretation, it would be helpful to be more explicit.

Fourth, continuing the above point more generally, it appears that every site on the internet must be moved behind an audited CDN or fronted by an audited proxy; sites not meeting this criteria will be blocked. It seems unlikely that the entire internet will move behind audited CDNs. It seems more likely that we will need to route a huge fraction of internet traffic through audited proxies. This is a huge part of the proposal yet it's not discussed at all -- who has the resources and motivation (incentives) to run such proxies?

Last, it's not clear what happens to sites like Netflix or Youtube which run their own CDNs out of necessity. Would users need an exception to access those sites?

[I don't have comment access so apologies if some of these are dups]

On Fri, Sep 13, 2019 at 11:33 AM Paul Jensen <pauljensen@google.com> wrote:
> On Fri, Sep 13, 2019 at 1:52 PM Alan Su <alsu@google.com> wrote:
> Paul, thanks for writing that up.
>
> The thanks go to lassey@.
>
> interesting concept! the part i'm having the hardest time wrapping my head around is how violations would be detected. i'm imagining an unscrupulous hosting service that builds up a sufficient amount of trust that is then able to violate the privacy budget for some undetectable fraction of the traffic it hosts. i see a lot of similarities between this concept and the SSL cert infrastructure, but in the latter, violations (i.e., CAs issuing bad certs) strike me as being much easier to detect and substantiate than in the former. did i miss something that addresses concerns such as this?

The "Policy Enforcement Mechanisms" section seeks to address this, but as you point out it's not foolproof. Fortunately, the consequences for violating IP privacy aren't nearly as harmful as violating certificate trust. Impersonating a bank for a small fraction of traffic is a big problem, but tracking only works when you can track lots of users across lots of sites, though I suppose this doesn't require a lot of traffic. I like to put it in relative perspective: the trust imbued by believing someone is enforcing IP privacy is similar to the trust imbued by believing a DNS resolver conforms to Mozilla's Trusted Recursive Resolver policy or Google Public DNS's privacy policy.

also, the point about IP-hiding flustering existing DoS detection mechanisms is a fascinating point that i had never thought of...

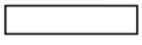
-alan

On Fri, Sep 13, 2019 at 7:58 AM Paul Jensen (via Google Docs) <pauljensen@google.com> wrote:

Paul Jensen has shared a link to the following document:

Willful IP Blindness

The latest proposal for a public explainer on the subject of IP address privacy.



Google Docs: Create and edit documents online.

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

You have received this email because someone shared a document with you from Google Docs.

--

You received this message because you are subscribed to the Google Groups "IP address privacy" group.
To unsubscribe from this group and stop receiving emails from it, send an email to ip-address-privacy+unsubscribe@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/ip-address-privacy/0000000000000801bd20592707d57%40google.com.

--

You received this message because you are subscribed to the Google Groups "IP address privacy" group.
To unsubscribe from this group and stop receiving emails from it, send an email to ip-address-privacy+unsubscribe@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/ip-address-privacy/CABQTWrmCLT%3D8L4_6Y%2ByBShx-T4af3BUU9ZrJTGZ-1FDL3-CVhA%40mail.gmail.com.

--

You received this message because you are subscribed to the Google Groups "IP address privacy" group.
To unsubscribe from this group and stop receiving emails from it, send an email to ip-address-privacy+unsubscribe@google.com.
To view this discussion on the web visit https://groups.google.com/a/google.com/d/msgid/ip-address-

privacy/CA%2B3%2Bx5E%3DpL6vBQ6qhDsZM6RhGzQCQqZ6CDFNs13idMWSgM2qgQ%40mail.gmail.com.